[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request an Extension from OMB of One Current Public Collection of Information: Cybersecurity Measures for Surface Modes

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day Notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently-approved Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652–0074, abstracted below, that we will submit to OMB for an extension in compliance with the Paperwork Reduction Act (PRA). On November 30, 2021, OMB approved TSA's request for an emergency approval of this collection to address the ongoing cybersecurity threat to surface transportation and associated infrastructure. TSA is now seeking to renew the collection, which expires on May 31, 2022, with incorporation of the subject of the emergency request. The ICR describes the nature of the information collection and its expected burden. The collection allows TSA to address the ongoing cybersecurity threat using a risk-based approach to transportation security.

DATES: Send your comments by [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Comments may be e-mailed to TSAPRA@tsa.dhs.gov or delivered to the TSA PRA Officer, Information Technology (IT), TSA-11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6011.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh at the above address, or by telephone (571) 227-2062.

SUPPLEMENTARY INFORMATION:

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation will be available at http://www.reginfo.gov upon its submission to OMB. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to--

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

OMB Control Number 1652-0074; Cybersecurity Measures for Surface Modes. Under the Aviation and Transportation Security Act[1] and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for "security in all modes of transportation . . . including security responsibilities . . . over modes of transportation that are exercised by the Department of Transportation."[2] TSA is

[1] Pub. L. 107-71 (115 Stat. 597; Nov. 19, 2001), codified at 49 U.S.C. 114.

[2] *See* 49 U.S.C. 114(d). The TSA Administrator's current authorities under the Aviation and Transportation Security Act have been delegated to him by the Secretary of Homeland Security. Section 403(2) of the Homeland Security Act (HSA) of 2002, Pub. L. 107-296 (116 Stat. 2135, Nov. 25, 2002), transferred all functions of TSA, including those of the Secretary of Transportation and the Under Secretary of Transportation of Security related to TSA, to the Secretary of Homeland Security. Pursuant to DHS Delegation Number 7060.2, the Secretary delegated to the Administrator of TSA, subject to the Secretary's

specifically empowered to assess threats to transportation;[3] develop policies, strategies, and plans for dealing with threats to transportation;[4] oversee the implementation and adequacy of security measures at transportation facilities;[5] and carry out other appropriate duties relating to transportation security.[6]

On November 30, 2021, OMB approved TSA's request for an emergency approval of this information collection that covers both mandatory reporting and voluntary reporting of information. The OMB approval allowed for the institution of mandatory reporting requirements and collection of information voluntarily submitted. *See* ICR Reference Number: 202111-1652-003. TSA is now seeking renewal of this information collection for the maximum three-year approval period.

The request for a new collection was necessary as a result of actions TSA took to address the ongoing and escalating cybersecurity threat to surface transportation and associated infrastructure. On December 2, 2021, TSA issued Security Directive (SD) 1580-2021-01 or SD1582-2021-02 mandating TSA-specified owner/operators of "higher risk" railroads and rail transit systems, respectively, to implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure.[7] The scope of these SDs align with the railroads and rail transit systems required to report significant security incidents to TSA under 49 CFR 1570.203.

On that same date, TSA also issued an "information circular" (IC), which contains non-binding recommendations with the same measures for railroad owner/operators,

---

guidance and control, the authority vested in the Secretary with respect to TSA, including that in section 403(2) of the HSA.

[3] 49 U.S.C. 114(f)(2).

[4] 49 U.S.C. 114(f)(3).

[5] 49 U.S.C. 114(f)(11).

[6] 49 U.S.C. 114(f)(15).

[7] Companies and agencies that are identified as higher-risk service the regions with the highest surface transportation-specific risk. Risk ranking is based on considerations related to ridership, location of services provided (use of the same stations and stops), and relationship between feeder and primary systems. *See* https://www.tsa.gov/sites/default/files/guidance-docs/high_threat_urban_area_htua_group_designations_0.pdf

public transportation agencies, rail transit system owner/operators, and certain over-the-road bus owner/operators not specifically covered under SDs 1580-2021-01 or 1582-2021-02. The requirements in the SDs and the recommendations in the IC allow TSA to execute its security responsibilities within the surface transportation industry, through awareness of potential security incidents and suspicious activities. The SDs require, and the IC recommends, the following security measures:

1. Designate a Cybersecurity Coordinator who is available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise;
2. Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA);
3. Develop a cybersecurity incident response plan; and
4. Complete a cybersecurity vulnerability assessment to address cybersecurity gaps using the form provided by TSA.

TSA, in conjunction with federal partners such as CISA, will use the reports of cybersecurity incidents to evaluate and respond to imminent and evolving cybersecurity incidents and threats as they occur, and as a basis for creating new cybersecurity policy moving forward. This monitoring will allow TSA and federal partners to take action to contain threats, take mitigating action, and issue timely warnings to similarly-situated entities against further spread of the threat. TSA and its federal partners will also use the information to inform timely modifications to cybersecurity requirements to improve transportation security and national economic security. TSA will use the collection of information to ensure compliance with TSA's cybersecurity measures required by the SDs and the recommendations under the IC.

Table 1 provides more detail on the measures included in the SDs and IC.

Table 1. Summary of Security Measures in the Security Directive and Information Circular

Title	Security Measure

Designate a Cybersecurity Coordinator	Owner/Operators are required or recommended, as applicable, to appoint a U.S. Citizen Cybersecurity Primary and Alternate Coordinator who must or should, as applicable, submit contact information. The Cybersecurity Coordinator serves as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA; must/should be accessible to TSA and CISA 24 hours a day, seven days a week; must/should coordinate cyber and related security practices and procedures internally; and must/should work with appropriate law enforcement and emergency response agencies.
Cybersecurity Incident Reporting	Owner/Operators Cybersecurity Coordinators are required or recommended, as applicable, to report actual and potential cybersecurity incidents to CISA within 24 hours of identification of a cybersecurity incident. The information provided to CISA pursuant to the SD is shared with TSA and may also be shared with the National Response Center and other agencies as appropriate. Conversely, information provided to TSA pursuant to this directive is shared with CISA and may also be shared with the National Response Center and other agencies as appropriate. Cybersecurity incident reports are submitted using the CISA Reporting System form at: https://us-cert.cisa.gov/forms/report. Incident reports can also be reported by calling (888) 282-0870. CISA has an approved information collection for cybersecurity incident reporting. *See* OMB control number 1670-0037.
Cybersecurity Incident Response Plan	Owner/Operators are required or recommended, as applicable, to develop and adopt a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should their Information Technology and/or Operational Technology systems be affected by a cybersecurity incident. Owner/operators must provide or are recommended to provide, as applicable, evidence of compliance to TSA upon request.
Cybersecurity Vulnerability Assessment	Owner/Operators are required or recommended, as applicable, to assess their current cybersecurity posture consistent with the functions and categories found in the National Institute of Standards and Technology Cybersecurity Guidance Framework. The assessment and identification of cybersecurity gaps must or should, as applicable, be completed using a using a form provided by TSA. As part of this assessment, the owners and operators must/may identify remediation measures to address the vulnerabilities and cybersecurity gaps identified during the assessment and a plan for implementing the identified measures if necessary, and report the results to TSA. TSA will use the results of the assessments to make a global assessment of the cyber risk posture of the industry and possibly impose additional security measures as appropriate or necessary. TSA may also use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and CISA may also use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

Certification of completion of SD requirements

The SDs and IC took effect on December 31, 2021. Within 7 days of the effective date of the SDs, owner/operators must provide their designated Cybersecurity Coordinator information; within 90 days of the effective date of the SDs owner/operators must complete the Vulnerability Assessment (TSA form); within 180 days of the effective date of the SDs, owner/operators must adopt a Cybersecurity Incident Response Plan; within 7 days of completing the Cybersecurity Incident Response Plan requirement, owner/operators must submit a statement to TSA via email certifying that the owner/operator has completed this requirement of the SD. Owner/Operators can

complete and submit the required information via email or other electronic options provided by TSA. Documentation of compliance must be provided upon request. As the measures in the IC are voluntary, the IC does not require owner/operators to report on their compliance.

Portions of the responses that are deemed Sensitive Security Information (SSI) are protected in accordance with procedures meeting the transmission, handling, and storage requirements of SSI set forth in 49 CFR part 15 and 1520.

TSA estimates this collection applies to 457 railroad owner/operators, 115 public transportation agencies and rail transit system owner/operators, and 209 over-the-road bus owner/operators, for a total of 781 respondents. TSA estimates the total hour burden for this collection to be 96,163 hours.

Dated: December 20, 2021.

Christina A. Walsh,

TSA Paperwork Reduction Act Officer,

Information Technology.

[FR Doc. 2021-27886 Filed: 12/22/2021 8:45 am; Publication Date: 12/23/2021]